



Berechtigungs- und Protokollierungssystem

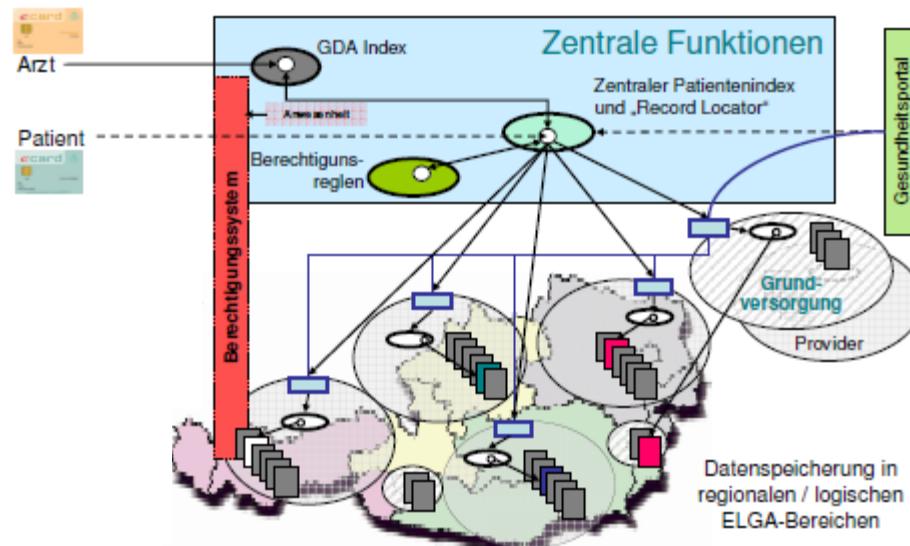
- Einleitung
- Zugriffsschutzmechanismus
- Anwendungsfälle

- Einleitung
- Zugriffsschutzmechanismus
- Anwendungsfälle

- Hintergrund
 - Umsetzung strikter Datenschutzvorgaben
 - Integrated Care EHR (vgl. ISO TR 20514)
„...mehreren, autorisierten Personen zugänglich...basierend auf Patienten-Zustimmung & Access-Policies“
- Flexibilität & Skalierbarkeit
 - Einsatz existierender Zugriffs-Kontroll Standards
 - Role-based Access-Control
- Transparenz
 - Verfügungsrecht bei Bürger → Wahrnehmung Opt-Out
 - Nachvollziehbarkeit sicherstellen
 - Akzeptanz fördern













- Einleitung
- **Zugriffsschutzmechanismus**
- Anwendungsfälle

- Berechtigungs- & Protokollierungssystem
 - Authentifizierung, Autorisierung, Protokollierung
 - ELGA Basiskomponente → Entscheidung zentral
 - Durchsetzung der Zugriffs-Regeln dezentral



- akkordiertes Rollen-Konzept als Voraussetzung
 - Personen: z.B. Arzt
 - sowie Institutionen: z.B. Krankenanstalt, Apotheke, Pflegeheim
- national
 - Rollen & Zugriffs-Rechte durch Gesetzesgeber definiert

Beispiel: Berechtigungsmatrix

Rolle	Laborbefund	Medikationsdaten	Zugriffsprotokoll
Arzt/Ärztin			
Apotheke			
Krankenhaus			
Patient			



read/write



read



no access

- Basis für Zugriffsentscheidungen
- Generelle Policies
 - durch Gesetzesgeber festgelegt
 - Rollen, Dokumentklassen, Aktionen
- Individuelle Policies
 - Möglichkeit individueller Spezifizierung
 - Priorität individueller gegenüber genereller Policies

1. ELGA Identity-Assertion

- bestätigt Identität & Rolle → elektr. Zertifikat
- Security Assertion Markup Language (SAML 2.0)

2. Zugriffs-Berechtigungen

- generelle/individuelle-Policies
- eXtensible Access Control Markup Language (XACML 2.0)
 - Kommunikation per SAML-Nachrichten
- Policy Administration, Decision & Enforcement Point

- Policy Administration Point - PAP
 - hält Zugriffs-Berechtigungen der ELGA-Nutzer
- Policy Decision Point - PDP
 - verarbeitet Identity Assertions & Berechtigungen
 - trifft Zugriffs-Entscheidung → allow/deny
- Policy Enforcement Point - PEP
 - setzt PDP-Entscheidung um

- Einleitung
- Zugriffsschutzmechanismus
- **Anwendungsfälle**

ELGA - Berechtigungssystem Ausstellung - Zugangsberechtigung Bürger



Bürgerkarte



Zugang zu den
persönlichen
Daten in ELGA



Einschau
eigene
Gesundheitsdaten

Festlegung
individuelle
Zugriffsregeln

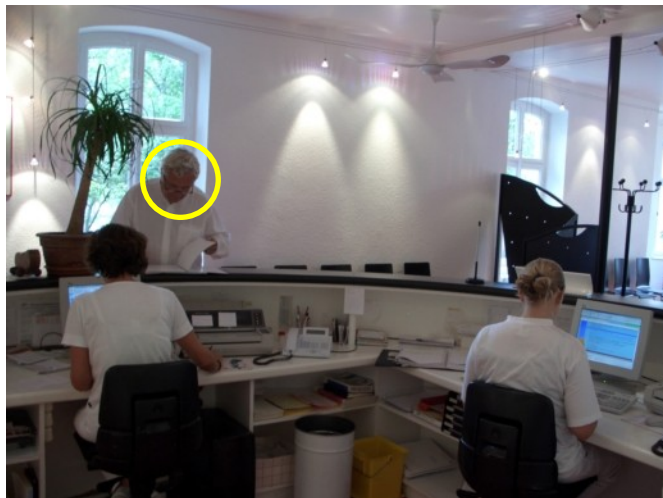


Ausstellung
Zugangsberechtigung



Einschau
Protokoll





Anmeldung am Arztsystem über:

- o-card mit Passwort oder
- Bürgerkarte mit Passwort oder
- anderen Identity-Provider

Anmeldung am ELGA-System

- mit bestätigter Identität

Bestätigung der aktuellen Rolle durch **ELGA-Berechtigungssystem** am GDA-Index

Zugang zur ELGA



Ausstellung
Zugangsberechtigung Arzt



ELGA - Berechtigungssystem

Ausstellung - Zugangsberechtigung Arzt 2



Auswahl Patient im System nach Erfüllung der Informationspflichten und Bestätigung des **Behandlungszusammenhanges**

Aufruf der generellen und der individuellen Zugriffsregeln durch **ELGA-Berechtigungssystem**

Ausstellung (mit oder ohne Einschränkungen) der Zugriffsberechtigungen für **diesen** Arzt auf die Gesundheitsdaten **dieses** Patienten



Patienten-Index



ELGA Dokumentenregister

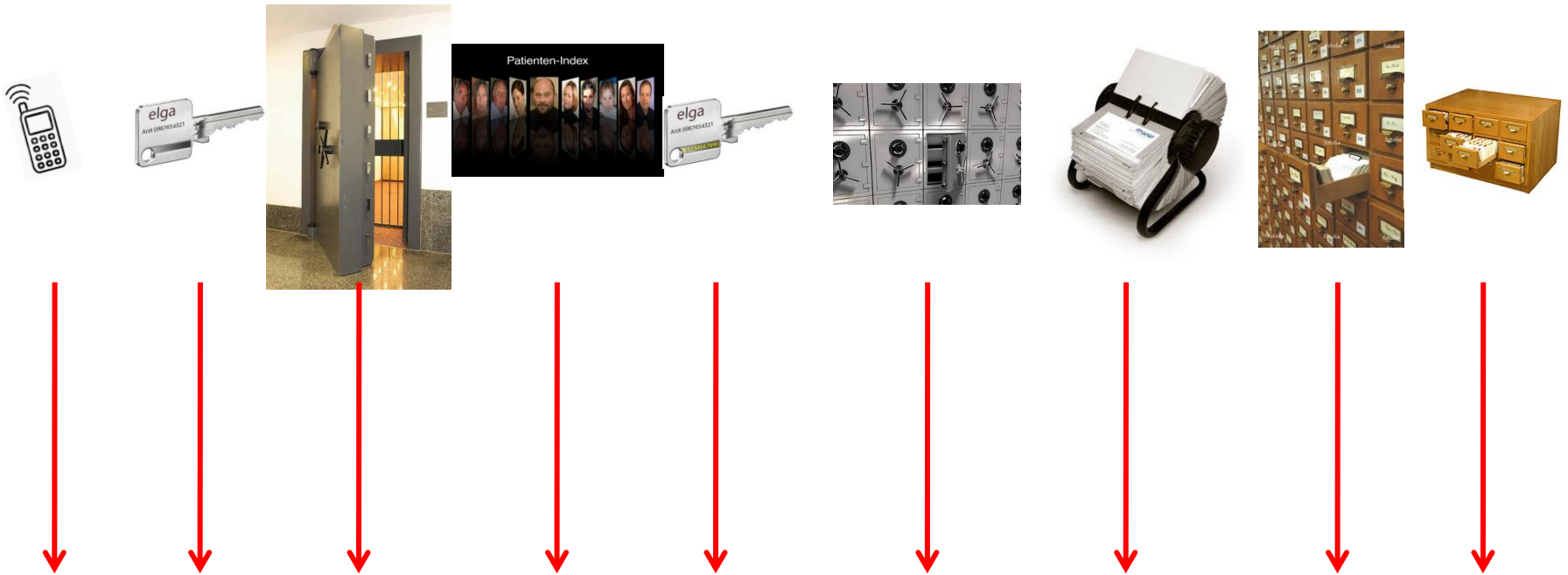


Krankenhaus xyz
Dokumente nach
KAKuG § 10



Ordination vwx
Dokumente nach
Ärztegesetz § 51





P r o t o k o l l i

überwacht; **fraud detection** im Rahmen des ISMS

Zugangsberechtigung Arzt-Patient Dokumentensuche und -abruf

